Free Questions for NSE5_FAZ-7.2 by ebraindumps

Shared by Rodriguez on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which log will generate an event with the status Contained?

Options:

A- An IPS log with action=pass.

B- A WebFilter log with action=dropped.

C- An AV log with action=quarantine.

D- An AppControl log with action=blocked.

Answer:

C

Question 2

Question Type: MultipleChoice

What are two benefits of using fabric connectors? (Choose two.)

Options:

A- They allow FortiAnalyzer to send logs in real-time to public cloud accounts.

B- You do not need an additional license to send logs to the cloud platform.

C- Fabric connectors allow you to improve redundancy.

D- Using fabric connectors is more efficient than using third-party polling with API.

Answer:

A, C

Question 3

Question Type: **MultipleChoice**

Why run the command diagnose sql status sqlplugind?

Options:

A- To list the current SQL processes running

B- To check what is the database log insertion status

C- To display the SOL query connections and hcache status

D- To view the current hcache size

Answer:

C

Question 4

Question Type: **MultipleChoice**

Which statement about the FortiSOAR management extension is correct?

Options:

A- It requires a FortiManager configured to manage FortiGate

B- It requires a dedicated FortiSOAR device or VM.

C- It does not include a limited trial by default.

D- It runs as a docker container on FortiAnalyzer

Answer:

D

Question 5

Question Type: MultipleChoice

Which item must you configure on FortiAnalyzer to email generated reports automatically?

Options:

A- Output profile

B- Report scheduling

C- SFTP server

D- SNMP server

Answer:

A

Question 6

Question Type: MultipleChoice

How can you attach a report to an incident?

Options:

A- By attaching it to an event handler alert

B- By editing the settings of the desired report

C- From the properties of an existing incident

D- Saving it in JSON format, and then importing it

Answer:

C

Question 7

Question Type: MultipleChoice

Which statement describes online logs on FortiAnalyzer?

Options:

A- Logs that reached a specific size and were rolled over

B- Logs that can be used to create reports

C- Logs that can be viewed using Log Browse

D- Logs that are saved to disk, compressed, and available in FortiView

Answer:

C

Question 8

Question Type: MultipleChoice

Why must you wait for several minutes before you run a playbook that you just created?

Options:

A- FortiAnalyzer needs that time to parse the new playbook.

B- FortiAnalyzer needs that time to back up the current playbooks.

C- FortiAnalyzer needs that time to ensure there are no other playbooks running.

D- FortiAnalyzer needs that time to debug the new playbook.

Answer:

A

Question 9

Question Type: MultipleChoice

What are two effects of enabling auto-cache in a FortiAnalyzer report? (Choose two.)

Options:

A- The size of newly generated reports is optimized to conserve disk space.

B- FortiAnalyzer local cache is used to store generated reports.

C- When new logs are received, the hard-cache data is updated automatically.

D- The generation time for reports is decreased.

Answer:

C, D

Question 10

Question Type: **MultipleChoice**

Which two statements are true regarding the outbreak detection service? (Choose two.)

Options:

A- New alerts are received by email.

B- Outbreak alerts are available on the root ADOM only.

C- An additional license is required.

D- It automatically downloads new event handlers and reports.

Answer:

C, D

Question 11

Question Type: MultipleChoice

What must you consider when using log fetching? (Choose two.)

Options:

A- The fetch client can retrieve logs from devices that are not added to its local Device Manager

B- You can use filters to include only logs from a single device.

C- The fetching profile must include a user with the Super_User profile.

D- The archive logs retrieved from the server become archive logs in the client.

Answer:

B, C

Question 12

Question Type: MultipleChoice

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

Options:

A- Incidents dashboards

B- Threat hunting

C- FortiView Monitor

D- Outbreak alert services

Answer:

B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.